AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1-9. (canceled)

10. (currently amended) A network attack detection system, comprising processors programmed to perform the steps of:

examining a header of a packet in transmission;

observing values of one or more pre-specified fields in the packet header; and

in a case where a number of distinct values observed in the pre-specified fields reaches a pre-specified threshold suggesting a pre-specified ratio within a pre-specified time interval, judging that an unauthorized attack is in progress[[,]];

wherein the judging is carried out based on one of the following conditions where N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1, P(t) is the number of packets in transmission within the pre-specified time interval from time t, $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and T(t) is the number of octets or bits in

the packets in transmission within the pre-specified time interval from some time t, then start listing the alternative conditions:

(a) ~~N(t) is the number of distinct values of the field observed within a pre specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre specified time interval from some time t_1, and~~ if the ratio of N(t) to $N(t_1)$ is greater than or equal to a first pre-specified threshold k_1, that is, if $N(t)/ N(t_1) \geq k_1$, the system will judge that an attack is in progress;

(b) ~~P(t) is the number of packets in transmission within the pre specified time interval from time t, and~~ if the ratio of ~~the number of~~ N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t)/P(t) \geq k_2$, the system will judge that an attack is in progress;

(c) ~~$P(t_1)$ is the number of packets in transmission within the pre specified time interval from some time t_1, and~~ if the ratio of ~~the coefficient computed in (b) above for the time t to that computed for the time t1,~~ $\{N(t)/P(t)\}$ [[/]] to $\{N(t_1)/P(t_1)\}$, is greater than or equal to a third pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geq k_3$, the system will judge that an attack is under progress; or

(d) ~~T(t) is the number of octets or bits in the packets in transmission within the pre specified time interval from some time t, and~~ if the ratio N(t) to T(t) is greater than or equal to

a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, the system will judge that an attack is in progress.

11. (currently amended) The network attack detection system according to claim 10, wherein ~~arbitrary combinations of two or more header fields are allowed, and the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold~~ the processors are further programmed to perform the further step of:

in a case where numbers of distinct values observed in the pre-specified fields, comprising arbitrary combinations of two or more header fields, reach a pre-specified threshold within a pre-specified time interval, judging that an unauthorized attack is in progress,

wherein the judging is carried out based on one of the above conditions (a)-(d).

12. (currently amended) The network ~~attach~~ attack detection system according to claim 10, wherein the processors are further programmed to perform the further step of:

in a case where ~~an illegal attack is inferred to be underway when~~ the Time To Live (TTL) value in the header field of [[a]] the packet does not lie in the range of the values seen

beforehand for the source address in the header field of ~~packets~~ the packet, judging that an unauthorized attack is in progress.

13. (currently amended) [[A]] The network attack detection system according to claim 10, wherein the processors are further programmed to perform the step of:

~~it is judged that an illegal attack has taken place by observing the values of the packet header fields, and when the number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, it is judged that an attack is in progress~~ in a case where numbers of distinct values observed in the pre-specified fields comprising of arbitrary combinations of two or more header fields are greater than, or equal to, one's pre-specified threshold value within a pre-specified time interval, judging that an unauthorized attack is in progress.

14. (currently amended) The network attack detection system according to claim 13, wherein the processors are further programmed to perform the step of:

in a case where ~~the judgment is made that an attack is in progress, if~~ the Time to Live (TTL) value in the header field of the packet does not lie in the range of the values seen beforehand for the source address in the header field of the packet, judging that an unauthorized attack is in progress.

15. (currently amended) ~~The~~ A network attack tracking system ~~according to claim 10~~, comprising:

two or more of the network attack detection systems as claimed as claim 10,

wherein a source of the unauthorized attack is searched by deploying ~~these systems~~ said two or more of the network attack detection systems at various places on the Internet.

16. (currently amended) ~~The~~ A network attack tracking system ~~according to claim 11~~, comprising:

two or more of the network attack detection systems as claimed as claim 11,

wherein a source of the unauthorized attack is searched by deploying ~~these systems~~ said two or more of the network attack detection systems at various places on the Internet.

17. (currently amended) ~~The~~ A network attack tracking system ~~according to claim 12~~, comprising:

two or more of the network attack detection systems as claimed as claim 12,

wherein a source of the unauthorized attack is searched by deploying ~~these systems~~ said two or more of the network attack detection systems at various places on the Internet.

18. (currently amended) ~~The~~ A network attack tracking system ~~according to claim 13~~, comprising:

two or more of the network attack detection systems as claimed as claim 13,

wherein a source of the unauthorized attack is searched by deploying ~~these systems~~ said two or more of the network attack detection systems at various places on the Internet.

19. (currently amended) ~~The~~ A network attack tracking system ~~according to claim 14~~, comprising:

two or more of the network attack detection systems as claimed as claim 14,

wherein the source of the unauthorized attack is searched by deploying ~~these systems~~ said two or more of the network attack detection systems at various places on the Internet.

20. (currently amended) A method for detecting a network attack, comprising the steps of:

examining ~~a pre-specified field in~~ a header of a packet in transmission ~~for distinct values~~; ~~and~~

observing values of one or more pre-specified fields in the packet header; and

~~determining that an unauthorized attack is in progress based on an observed number of distinct values in the examined~~

~~pre-specified header field reaching a pre-specified threshold within a pre-specified time interval, wherein,~~ in a case where a number of distinct values observed in the pre-specified field reaches a pre-specified threshold suggesting a pre-specified ratio within a pre-specified time interval, judging that an unauthorized attack is in progress;

~~the determination includes that at least one of the following conditions is satisfied~~

wherein the judging is carried out based on one of the following conditions where N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_2)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_2, P(t) is the number of packets in transmission within the pre-specified time interval from time t, $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_2, and T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t , then start listing the alternative conditions:

(a) ~~N(t) is the number of the distinct values of the field observed within the pre specified time interval from some time t, $N(t_2)$ is the number of distinct values of the field observed within the pre specified time interval from some time t_2~~ and if the ratio of N(t) to $N(t_2)$ is greater than or equal to a

first pre-specified threshold k_1, that is $N(t)/N(t_1) \geq k_1$, it will be judged that an attack is in progress[[,]]; ;

(b) ~~P(t) is the number of packets in transmission within the pre-specified time interval from some time t, and~~ if the ratio of N(t) to P(t) is greater than or equal to a second pre-specified threshold k_2, that is, $N(t)/P(t) \geq k_2$, it will be judged that an attack is in progress[[,]]; ;

(c) ~~$P(t_2)$ is the number of packets in transmission within the pre-specified time interval from the time t_1, and~~ if the ratio of ~~the coefficient computed in (b) above for the time t to that computed for the time t1,~~ {N(t)/P(t)} [[/]] to $\{N(t_2)/P(t_2)\}$[[,]] is greater than or equal to a third pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_2)\} \geq k_3$, it will be judged that an attack is in progress[[,]]; ~~and~~ or

(d) ~~T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and~~ if the ratio N(t) to T(t) is greater than or equal to a fourth pre-specified threshold k_4, that is, $N(t)/T(t) \geq k_4$, it will be judged that an attack is in progress.

21. (currently amended) The method ~~of~~ according to claim 20, ~~wherein,~~ further comprising the step of:

~~said examining step examines a resultant composite field comprising arbitrary combinations of two or more of header fields, and~~

~~the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold~~

in a case where numbers of distinct values observed in the pre-specified fields, comprising of arbitrary combinations of two or more header fields, reach a pre-specified threshold within a pre-specified time interval, judging that an unauthorized attack is in progress,

wherein the judging is carried out based on one of the above conditions (a)-(d).

22. (currently amended) The method ~~of~~ according to claim 20, comprising the further ~~steps~~ step of:

in a case where ~~from an examined packet, inferring that the unauthorized attack is underway when~~ a Time To Live (TTL) value in the ~~pre-specified~~ header field of the ~~examined~~ packet ~~is outside a~~ does not lie in the range of the values seen beforehand for the source address in the header field of the ~~examined~~ packet, ~~and after determining that the source address in the header of the examined packet is legitimate, detecting the unauthorized attack based on whether the TTL value is within a~~

~~pre-specified range of the expected TTL value for the source address~~ judging that an unauthorized attack is in progress.

23. (canceled)

24. (previously presented) [[A]] The method ~~for detecting a network attack~~ according to claim 20, further comprising the step of:

~~observing values of packet header fields and upon observing that a number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, judging that an unauthorized attack is in progress~~

in a case where numbers of distinct values observed in the pre-specified fields comprising of arbitrary combinations of two or more header fields are greater than, or equal to, one's pre-specified threshold value within a pre-specified time interval, judging that an unauthorized attack is in progress.

25. (currently amended) The method ~~of~~ according to claim 24, further comprising the step of:

in a case where ~~wherein a~~ the Time To Live (TTL) value in the ~~packet~~ header field of the packet ~~is observed, and the unauthorized attack in progress is judged upon the observed TTL value being outside a~~ does not lie in the range of the values

seen beforehand for the source address in the ~~packet~~ header field of the packet, judging that an unauthorized attack is in progress.

26. (canceled)